Testimony Of

D. JAMES BIDZOS

VICE CHAIR

SECURITY DYNAMICS TECHNOLOGIES, INC.
PARENT COMPANY OF RSA DATA SECURITY, INC.

On Behalf Of

AMERICANS FOR COMPUTER PRIVACY

IMMEDIATE NEED FOR RELAXATION OF EXPORT CONTROLS FOR SOFTWARE AND HARDWARE WITH ENCRYPTION CAPABILITIES

Before The

COMMERCE, SCIENCE AND TRANSPORTATION COMMITTEE

OF THE

U.S. SENATE

Washington, D.C.

June 10, 1999

SUMMARY OF STATEMENT OF D. JAMES BIDZOS
VICE CHAIR OF SECURITY DYNAMICS TECHNOLOGIES, INC.

Congress must immediately relax export controls on software and hardware with encryption capabilities. Widespread deployment of American products with encryption capabilities will help to accelerate dramatically the growth of electronic commerce by protecting consumers' privacy and preventing electronic crime.

Without relaxation of export controls, U.S. manufacturers remain at a competitive disadvantage, and foreign consumers will purchase encryption products from foreign suppliers. Foreign products are comparable in capabilities and quality. When a foreign purchaser cannot obtain an American product they simply purchase it from a foreign supplier. Unfortunately, not only are American companies losing a sale of an encryption item, but they are also losing the sale of the program or hardware such as an Internet server or an application browser that uses the encryption capability. In fact, companies risk losing sales of entire systems because of their inability to provide necessary security features. The only impact of the Administration's export policy is widespread deployment of foreign designed and manufactured software and hardware.

The Administration took the first step towards developing a sensible long-term encryption policy by permitting exports of select products to select users, but they still have not gone far enough.

The PROTECT Act is an improvement over current Administration policy. It affirms that Americans may use and sell any type of encryption domestically, and ensures that the U.S. Government may not use its full powers and capabilities to compel Americans to use or sell a certain type of encryption. The PROTECT Act also provides a broader range of export relief for American encryption products and provides a certain timeframe for the export review process. Also, the Act provides Congressional support for, and sets a 5-year limit on the selection of, the 128-bit Advanced Encryption Standard.

The PROTECT Act should be further improved to reflect market and technological realities. The PROTECT Act does not permit individual foreign consumers to obtain strong, non-recoverable encryption, making it impossible for them to securely purchase products from American companies. Also, the Act does not provide immediate export relief for encryption sales to small businesses – one of the fastest growing worldwide business sectors.

Unfortunately, the PROTECT Act limits easy exportability of mass market products with strong 128-bit encryption until NIST adopts the Advanced Encryption Standard. This means individual consumers and small businesses will have to wait three years to obtain strong American encryption, and foreign companies will have had three more years to market their products. Exportability in the meantime is dependent on an unwieldy complex bureaucracy that will determine whether American products are generally available or compete with comparable foreign products. We believe the evidence already is overwhelming regarding these facts.

Introduction

Good Morning. My name is Jim Bidzos, and I am Vice Chair of Security Dynamics Technologies, Inc., a Massachusetts-based security firm that is also the parent company of RSA Data Security, located in San Mateo, California. For over 13 years, until earlier this year, I was the President and CEO of RSA Data Security, the world's leading encryption company.

RSA's technology is embedded in both Netscape and Microsoft browsers, and in over 500 other products, all used by hundreds of millions of people around the world to secure internet transactions and digital data of many types. Over many years, I have personally negotiated hundreds of licenses to RSA encryption technology, including licenses with companies such as IBM, Microsoft, ATT, Netscape, Oracle, and Motorola. These negotiations almost always involve discussions about encryption needs, end-user requirements, and export policy. I have thus gained unique insights into the needs and concerns of both industry and users with respect to encryption.

I am also founder and chairman of Verisign, Inc., the leader in Internet authentication. Verisign is the world's largest Internet security products and services company as measured by both customers and market capitalization.

I am a member of the board of directors of several other security companies. One specializes in virtual private networks. Another is a manufacturer of security tokens. Another offers cryptographically secure digital time stamping services. I am also a director of a UK-based encryption hardware company, a Dublin-based secure electronic payments company, and two Japanese security companies.

I have been deeply involved in the debate over encryption, from many aspects, including US policy on the export of this technology. Over the last 13 years, I have testified many times before both the House and Senate on encryption policy, and I have participated in numerous US and international standards activities.

I believe that my long and unique history in the encryption area allows me to offer testimony today that may help the committee better understand industry's concerns over US encryption policy.

On behalf of Americans for Computer Privacy ("ACP"), thank you for the opportunity to testify on S.798, the PROTECT Act, sponsored by Chairman McCain and cosponsored by four other committee members Senators Burns, Wyden, Abraham, and Kerry.

ACP is a coalition of over 3,500 individuals, 40 trade associations and over 100 companies representing financial services, manufacturing, high-tech, and transportation industries as well as law enforcement, civil-liberty, taxpayer and privacy groups. ACP supports policies that allow American citizens to continue using strong encryption without government intrusion, and advocates the lifting of export restrictions of U.S. made encryption products.

But we really are here today to speak on behalf of the tens of millions of users of American software and hardware products. The American software and hardware industries have

succeeded because we have listened and responded to the needs of computer users worldwide. We develop and sell products that users want and for which they are willing to pay.

One of the most important features computer users are demanding is the ability to protect their electronic information and to interact securely worldwide. American companies have innovative products which can meet this demand and compete internationally. But there is one thing in our way – the continued application of overbroad, unilateral, export controls by the U.S. Government.

At the outset, I want to say that the PROTECT Act definitely moves us in the right direction and is a significant improvement over the Administration's current policy – but it could be further improved in several important respects (along the lines of the SAFE Act).

ACP recognizes a legitimate governmental need to obtain access to information and communications when authorized by proper legal authority. ACP and its members are responsible citizens. We have no wish to facilitate the commission of crime or the spread of terrorism. Similarly, we are committed to strengthening the nation's infrastructure and promoting national security, enhancing the privacy of American citizens and ensuring the security of electronic commerce.

But we believe that the best way of meeting all these objectives is promote the widespread use of encryption!

Ultimately, any truly successful, sensible encryption policy that has America's best interests at heart must be based on technological and market realities, and should not create winners and losers in the encryption marketplace on a sector-by-sector basis. It would recognize that:

- The worldwide encryption standard is 128-bit encryption;
- Mass market software and hardware is inherently uncontrollable; and
- It is in America's national and economic security interests to have American designed and manufactured encryption products deployed worldwide.

We believe it is preferable for Congress to put encryption policy on a statutory basis rather than continuing to leave it up to inconsistent Administration regulations – sending a strong message around the world that encryption is important for protecting the privacy of citizens, for promoting e-commerce, preventing crime and protecting our critical infrastructures and national defense.

The American Computer Software and Hardware Industries – An American Success Story

The computer software and hardware industries are American success stories, but they are being threatened. America's software and hardware industries are important contributors to U.S. economic security. Information technology industries now are directly responsible for over one-third of real growth of the U.S. economy, and both the computer and software industries are continuing to grow. From 1990 through 1996, the software industry grew at a rate of 12.5%, nearly 2.5 times faster than the overall U.S. economy.

More than 7 million people work in IT industries. In 1996, the software industry provided a total of over 619,000 direct jobs and $7.2 billion in tax revenues for the U.S. economy. The software industry is expected to create an average of 45,700 new jobs each year through 2005. If piracy were to be eliminated in the United States, the number of new software jobs created would double to an average of 93,000 a year.

Moreover, the computer software industry has achieved tremendous success in the international marketplace with global sales of packaged (*i.e.*, non-custom) software reaching over $118.4 billion in 1996, and rising to $135.4 billion in 1997. American produced software accounts for 70% of the world market, with exports of U.S. programs constituting half of the industry's output.

The incredible growth of the industry and its exporting success benefits America through the creation of jobs here in the United States. Many of these jobs are in highly skilled and highly paid areas such as research and development, manufacturing and production, sales, marketing, professional services, custom programming, technical support and administrative functions. In the U.S. software industry, workers enjoy more than twice the average level of wages across the entire economy – $57,319 versus $27,845 per person.

All of these revenues and jobs are dependent upon American software and hardware producers remaining the market leaders around the world, especially as the major growth markets continue to be outside the United States. Strong export controls on products with encryption capabilities are crippling the ability of these companies to compete with foreign providers and are only ensuring that foreign products are securing worldwide critical infrastructures, not American products.

Secure Networks And Confidential Information In The Internet Age Are The Key To Privacy And Commerce

American individuals and companies are rapidly becoming networked together through private local area networks (LANs), wide area networks (WANs) and public networks such as the Internet. Combined, these private and public networks are the economic engine driving electronic commerce, transactions and communications. This engine is sputtering and threatens to stall.

Traffic on the Internet doubles every 100 days. Predictions of business-to-business Internet commerce for the year 2000 range from $66 billion to $171 billion, and by 2002, electronic commerce between businesses is expected to reach $300 billion. During 1997, one

leading manufacturer of computer software and hardware sold $3 million per day online for a total of $1.1 billion for the year.

More and more individual consumers also are going on line and spending. Five years from today, we anticipate nearly 60 percent of all Americans to be using the Internet. More than 10 million people in North America alone have already purchased something over the Internet, and at least 40 million have obtained product and price information on the Internet only to make the final purchase off-line. Altogether last year, consumers spent nearly $8 billion online. Nearly 1.5 million Americans join the online population every month, and the number of worldwide online users is expected to reach 248 million by 2002.

The incredible participation by American consumers in the Internet phenomenon clearly demonstrates that the need for strong encryption is no longer merely the purview of our national security agencies concerned about securing data and communications from interception by foreign governments. Today, every American even merely dabbling on the Internet requires access to strong encryption. Imagine the boost in volume of e-commerce if all of these consumers had enough confidence in the security of the Internet to purchase on-line. Yet in 1996 the Computer Security Institute/FBI Computer Crime Survey indicated that our worldwide corporations will be increasingly under siege: over half from within the corporation, and nearly half from outside of their internal networks.

Network users ***must*** have confidence that their communications and data – whether personal letters, financial transactions or sensitive business information – are secure and private. Electronic commerce is transforming the marketplace – eliminating geographic boundaries and opening the world to buyers and sellers. Companies, governments and individuals now realize that they can no longer protect data and communications from others by relying on limiting physical access to computers and maintaining stand-alone centralized mainframes. Instead, users expect to be able to pick up their e-mail or modify a document from any computer anywhere in the world simply by using their Internet browsers. Thus, consumers worldwide are demanding to be able to protect their electronic information and interact securely worldwide, and access to products with strong encryption capabilities has become critical to providing them with confidence that they will have this ability.

Unilateral U.S. Export Controls Harm American Interests

Currently, there are no restrictions on the use of cryptography within the United States. However, the U.S. Government maintains strict ***unilateral*** export controls on computer products that offer strong encryption capabilities.

American companies are forced to limit the strength of their encryption to the 56-bit key length level set late in 1998. The recently announced regulations will also permit companies to export stronger encryption on a sector-by-sector, user-by-user basis. However, this policy ignores the fact that:

- The minimum strength now required by new Internet applications is 128-bit encryption;
- American companies cannot export encryption products to a vast majority of non-U.S. commercial entities. Foreign manufacturers provide 128-bit encryption alternatives and add-ons – filling the market void created by U.S. export controls;
- Providing sector-by-sector relief is unworkable for mass market products and does not reflect commercial realities for sales of custom products;
- 56-bit encryption has been demonstrated to be vulnerable to commercial let alone governmental attack. (In the beginning of this year at the RSA Encryption Conference, a 56-bit DES encoded message was broken by private companies and individuals working together in 22 hours and 15 minutes – imagine what a hostile government with serious resources could do); and
- New developments in technology are introduced everyday that speed up decryption time. Adi Shamir, the Israeli computer scientist who is the "S" in RSA, recently announced "Twinkle", which is a proposed method for quickly unscrambling computer-generated codes that have until now been considered secure, at the International Association for Cryptographic Research's latest meeting in Prague.

The Wassenaar Arrangement Is Not A Multilateral Agreement To Control Encryption

I want to take one minute to discuss the Wassenaar Arrangement at this point. Please do not be fooled by any claims from the Administration that the Wassenaar Arrangement is the multilateral agreement on encryption that they have been touting was just around the corner for the past several years.

The Wassenaar Arrangement replaced the old COCOM regime with a non-binding agreement among 30 countries to report on their sensitive exports. The December 1998 Wassenaar Arrangement agreement actually decontrolled encryption products. Many countries, such as Israel and South Africa, who export strong encryption are not signatories to the Arrangement. The Wassenaar Arrangement eliminates controls of any sort on 56-bit encryption and permits exports of up to 64-bit encryption in mass-market software and hardware. It also removed any reporting requirements – the sole official means for actually monitoring what countries are doing. Although the Arrangement left open the possibility that countries might

individually control 128-bit encryption, we are skeptical that they will do so. There is no penalty for failing to control 128-bit encryption, and most countries are actually moving towards *encouraging* the use of stronger encryption. Finally, a country could technically comply with the Arrangement, while still permitting easy exports of strong encryption.

Ironically, the U.S. government is a good example of the lack of effect of the Wassenaar Arrangement. In its new encryption regulations, the Administration is still controlling encryption products with greater than 56, not 64, bit keys, and they have imposed reporting requirements on mass market products even if they are using 64-bit encryption.

Recently, on June 2, 1999, the German government established a new encryption policy seeking to improve protection of German users of global information networks and clarifying that any encryption product may be developed, produced marketed and used without restrictions in Germany. The German government declared its intention to simplify their export review process and to strengthen the performance and ability of German manufacturers to compete internationally. The German government will monitor abuses of encryption for illegal purposes and attempt to further improve the technical capabilities of German law enforcement and security agencies to handle advances in encryption technology.

Even France, traditionally the country which placed the greatest restrictions on its own citizens by limiting them to the easily broken 40-bit level of encryption, has recognized that technology has progressed. Near the end of 1998, France relaxed controls on the domestic use of encryption and is now permitting, and in fact encouraging, the use of 128-bit encryption by its citizens.

Without Export Relief, Foreign Consumers Will Purchase Their Products From Foreign Suppliers, Keeping U.S. Manufacturers At A Competitive Disadvantage

Export controls also have made American companies less competitive and opened the door for foreign software and hardware developers to gain significant market share –decreasing our national and economic security.

As a result of U.S. unilateral export controls, encryption expertise is being developed off-shore by foreign manufacturers who now provide hundreds of encryption alternatives and add-ons. The Administration's export controls are in no way preventing foreigners, let alone those with criminal intent, from obtaining access to encryption products. In fact, foreign software and hardware manufacturers have seized the opportunity to create sophisticated encryption products and to capture sales.

As long ago as 1995, the General Accounting Office confirmed that sophisticated encryption software is widely available to foreign users on foreign Internet sites. In 1996, a Department of Commerce study again confirmed the widespread availability of foreign manufactured encryption programs and products. Professor Hoffman today releases the results of his latest survey which shows the continuing growth in foreign encryption products in the face of U.S. export controls.

If an encryption product is combined with other applications such as Internet

browsers and application servers, U.S. companies generally will lose both sales. In fact, companies risk losing sales of entire systems because of inability to provide necessary security features. This permits foreign manufacturers to gain entry into companies as well as gain credibility – providing the foreign manufacturers with further opportunity to take away future sales in the same and other product lines.

U.S. Encryption Export Controls Hurt American Companies Without Helping Law Enforcement Or National Security

U.S. export controls have had the effect of creating an encryption expertise outside the United States that is gathering momentum. Unfortunately, every time research and development of an encryption technique or product moves off-shore, U.S. law enforcement and national security agencies lose. We believe that continuing down this path will be ultimately more harmful to our national security and law enforcement efforts as American companies will no longer be the world leaders in creating and developing encryption products.

In fact, as long ago as 1996, the NRC Committee concluded that as demand for products with encryption capabilities grows worldwide, foreign competition could emerge at levels significant enough to damage the present U.S. world leadership in information technology products. The Committee felt it was important to ensure the continued economic growth and leadership of key U.S. industries and businesses in an increasingly global economy, including American computer, software and communications companies. Correspondingly, the Committee called for an immediate and easy exportability of products meeting general commercial requirements – which is currently 128-bit level encryption!

To summarize:

- Foreign competitors not subject to outdated U.S. export controls are ready to take sales and customers from U.S. companies today.

- Complex and cumbersome U.S. export controls make American companies less competitive. They significantly increase the costs of developing, marketing and selling products with encryption capabilities, delay the introduction of new products or features, and encourage foreign customers to purchase from foreign suppliers due to the uncertainty and delay in obtaining a comparable American product.

- Current export controls do not keep strong encryption out of the hands of foreign customers; they just keep U.S. products out of their hands.

- In the future, if export controls on encryption are not relaxed, both American and foreign infrastructures will be secured by foreign encryption products, creating a significant problem for American law enforcement and national security

agencies.

American companies do have exciting and innovative products that can meet the demand for 128-bit encryption and compete internationally. But unless the current unilateral U.S. export restrictions are changed to allow the use of strong encryption, American individuals and businesses will not be active participants in this new networked world of commerce – let alone continue to be the leaders in its development. Furthermore, American companies will no longer be providing the world, and its critical infrastructures, with the answers to their security problems. Instead foreign companies will. It is unclear how U.S. national security or law enforcement will be aided or how our critical infrastructures will be secure when foreign encryption products dominate the world market.

The Bernstein Case

The absurdity of the existing export control regime is further highlighted by the recent decision of the 9th Circuit Court of Appeals in *Bernstein v. DOJ*. In that case, the court held that the existing restrictions on the export of source code, the language in which programmers communicate their ideas to one another, are an unconstitutional prior restraint on first amendment rights of free speech. So now we have a situation where it is permissible to export jobs (because one can export source code to teach foreign programmers), but not American products (because one cannot embody that source code in a product)!

More generally, Judge Fletcher's opinion raises some very valid, more general questions and points out how important encryption is to the mainstream life of Americans rather than merely to obscure technologists. Judge Fletcher states:

> In this increasingly electronic age, we are all required in our everyday lives to rely on modern technology to communicate with one another. This reliance on electronic communication, however, has brought with it a dramatic diminution in our ability to communicate privately. Cellular phones are subject to monitoring, email is easily intercepted, and transactions over the internet are often less than secure. Something as commonplace as furnishing our credit card number, social security number, or bank account number puts each of us at risk. Moreover, when we employ electronic methods of communication, we often leave electronic "fingerprints" behind, fingerprints that can be traced back to us. Whether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost. Government efforts to control encryption thus may well implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption's bounty. Viewed from this perspective, the government's efforts to retard progress in cryptography may implicate the Fourth Amendment, as well as the right to speak anonymously, . . . , the right against compelled speech, . . . , and the right to informational privacy. While we leave for another day the resolution of these difficult issues, it is important to point out that Bernstein's is a suit not merely

concerning a small group of scientists laboring in an esoteric field, but also touches on the public interest broadly defined.

The Administration Took a Small First Step Towards Developing A Sensible Long-Term Encryption Policy, But They Still Have Not Gone Far Enough.

Progress was made last year in the new Administration policy announced by the Vice President in September and contained in the interim final regulations of December 31, 1998.

ACP welcomed the Administration's efforts to relax export controls on select products used by select users. We especially appreciated the Administration's apparent abandonment of its key escrow policy that would have required all encryption exports (except for 40-bit and less encryption) to be capable of providing third parties with immediate access to the plaintext of stored data or communications without the knowledge of the user. Foreign companies and consumers simply would not purchase such products as a multitude of foreign products without key escrow are readily available.

However, the Administration's actions are merely a first step. U.S. export controls still ignore the realities of mass-market software and hardware distribution. Mass-market software publishers and hardware manufacturers sell products through multiple distribution channels such as OEMs (*i.e.*, hardware manufacturers that pre-load software onto computers), value-added resellers, retail stores and the emerging channel of on-line distribution. Thus, mass market products are available to the general public from a variety of sources. (It also is why continued reporting requirements about end-uses and end-users make no sense.)

The mass-market distribution model presupposes that software publishers and hardware manufacturers will take full advantage of these multiple channels to ship identical or substantially similar products worldwide (allowing only for differences resulting from localization) irrespective of specific customer location or characteristics. As mass market products are uncontrollable, ACP believes U.S. companies should be able to export the current market standard of 128-bit encryption. Unfortunately, the Administration has only proposed permitting easy exports of 56-bit encryption even if foreign products exist in the marketplace.

ACP also believes that encryption hardware and software should be treated identically. However, contrary to the Administration's original announcement regarding export relief which included export relief for hardware, the new regulations still do not permit 56-bit encryption chips, integrated circuits, toolkits and executable or linkable modules to be easily exported except to subsidiaries of U.S. companies or otherwise relax export controls on stronger mass market hardware.

In addition, ACP believes that the new regulations are so complex and contain unrealistic requirements that they undermine many of the benefits of the Administration's export relief for stronger encryption, especially for mass market hardware and software. U.S. companies are now required to meet a number of new, unilateral reporting requirements. For example, exporters now are required to report the name and address of end-users, a virtual impossibility for mass-market exporters because registration of end-users is customarily voluntary. A system to obtain the names and addresses of each of the millions of potential health care end-users, for example, would cost more than the profits yielded from many products.

ACP also is disappointed that the Administration's regulations do not clearly provide online merchants with the level of export control relief originally envisioned as they do not permit ISPs to provide "services" as a permissible end-use. This could chill the use by ISPs located abroad of U.S.-origin encryption products for billing, payment, and delivery purposes, despite the widespread foreign availability of such products.

The PROTECT Act Is An Improvement Over Current Administration Policy

The PROTECT Act Establishes The Correct Domestic Encryption Policy

The PROTECT Act affirms that Americans may use and sell any type of encryption domestically. Even more importantly, the PROTECT Act ensures that the U.S. Government may not use its full powers and capabilities to compel, directly or indirectly, Americans to use or sell a certain type of encryption. This will prevent the U.S. Government from attempting to achieve domestic controls on encryption through regulations or "incentives".

For example, the Act prohibits the U.S. Government from linking the ability to electronically sign a document to a requirement that the consumer use a particular encryption methodology for ensuring confidentiality. Thus, the U.S. Government cannot require Americans to use a certain type of encryption (such as key escrow) to engage in electronic commerce.

Also, the PROTECT Act specifically restricts the government from requiring any American to use a particular encryption product or methodology to communicate with or transact business with the government. The U.S. Government may only specify technologies for its own internal uses.

The PROTECT Act Provides Additional Export Relief For Encryption Products

The PROTECT Act provides a broader range of export relief for American encryption products than the Administration. We are pleased that the PROTECT Act provides immediate export relief after a one-time review by the government for:

- All encryption products using key lengths of 64-bits or less rather than the less secure 56-bit key lengths proposed by the Administration;
- All recoverable encryption products regardless of key length, including telecommunications related products; and
- All encryption products using key lengths greater than 64-bits to certain legitimate and responsible commercial users, including publicly traded firms, firms subject to government regulation, U.S. companies' foreign subsidiaries, affiliates and strategic partners, on-line merchants who use encryption products to support electronic commerce, and foreign governments who are members of NATO, OECD and ASEAN.

We are also pleased that the PROTECT Act recognizes the need for a quicker and more certain timeframe for the export review process. Businesses simply cannot live with the U.S. Government taking between 3 to 6 months to determine whether a product is exportable when many Internet products have 90 day product cycles and most businesses do not want to wait through one or two business quarters to update their computer systems.

The PROTECT Act Begins To Recognize Mass Market Product Realities

We also are encouraged that the PROTECT Act recognizes the difficulties in complying with reporting requirements for mass market encryption products and eliminates such reporting requirements. It is virtually impossible for mass-market exporters to report the name and address of each end-user. Millions of these products are sold through multi-level distribution channels (*e.g.*, VAR's and chain stores). Moreover, as registration of mass market products is customarily voluntary. This is a vast improvement over the Administration's proposed regulations which effectively require companies to develop a system to obtain the names and addresses for each health and medical end-user of stronger encryption products and all foreign online merchants.

The PROTECT Act also provides Congressional support for, and sets a 5-year limit on the selection of, the 128-bit Advanced Encryption Standard which is being developed under the auspices of the National Institute of Standards and Technology. The 2002 deadline will provide impetus for NIST to finish developing the standard in a timely manner while providing NIST with sufficient time to study the final standard's security features. This is an important process that will result in a new standard for government's sensitive, but unclassified, information and most likely will serve as the new worldwide standard for strong encryption

similar to the Data Encryption Standard when it was introduced in the 1970's. Once the algorithm is selected, the PROTECT Act removes all export controls on encryption products using the 128-bit standard or its equivalent strength.

The PROTECT Act Should Be Further Improved To Reflect Market And Technological Realities

The PROTECT Act Does Not Provide Immediate Export Relief For Individual Consumers

The PROTECT Act does not go far enough to protect the millions and millions of consumers that are now engaging in electronic commerce. Foreign consumers still will not be able to obtain an American Internet browser with strong, non-recoverable encryption, making it impossible for them to securely purchase products from American companies. Also, an everyday foreign consumer who wants to protect an on-line diary, copies of health care records or a business proposal, may not easily obtain strong encryption to do so from American sources if any portion of the encryption used by the product is non-recoverable. Under the bill, all these individuals must wait until 2002.

The PROTECT Act Does Not Provide Immediate Export Relief For Small Businesses

We believe the PROTECT Act provides greater export relief for larger corporate customers. However, until 2002, small and privately-owned businesses face significant difficulty in easily obtaining U.S. encryption under any of the License Exceptions established by the PROTECT Act. So, for example, if two doctors in private practice together in Brazil or a restaurant owner in France or a small shopping market in Germany wants to purchase non-recoverable encryption, these small businesses probably would purchase a comparable foreign product as an American company could not easily export it to them.

Unfortunately, as companies install the security "plumbing" into their individual computers and company networks, it becomes increasingly difficult for American companies to replace the foreign software and hardware that already has been installed. Because the small business sector is, and most likely will continue to be, the fastest growing business sector, this puts American companies at a distinct disadvantage in selling encryption products at a later date.

The PROTECT Act's Export Relief For Mass Market Products And For Products Which Face Competition From Comparable Foreign Products Is Too Complicated And Creates An Unwieldy Bureaucracy

The PROTECT Act does recognize that mass market and publicly available encryption products, and encryption products for which comparable foreign products are available, should be treated differently under the U.S. export regime. The bill acknowledges the futility of trying to control a product that can be bought off of the Internet or easily purchased from commercial vendors such as CompUSA or from Circuit City by any individual in America regardless of nationality, or a comparable product can be easily purchased from similar stores in a foreign country. "Bad guys" certainly will have no problems obtaining the encryption products, and no concerns about "exporting" the products via telephone lines or the Internet or smuggled out on personally pressed CDs. The only impact of the export controls will be to stop American companies from selling American products to legitimate users.

Unfortunately, the PROTECT Act establishes a complicated private/public board structure for deciding after-the-fact whether or not a product is a mass market product or whether comparable foreign products are available. The Secretary of Commerce has thirty days to approve or disapprove the Board determination, subject to judicial review, and the President may override any determination. Unfortunately, there is no guarantee of any consistency in the Board's decisions. Thus, while the Board procedure is an improvement, and the opportunity for judicial review provides a mechanism to ensure that exports are not denied in an arbitrary and capricious manner, it is not a predictable, clear process giving American companies certainty as to whether they can export their products. Such predictability is necessary so that American companies can have confidence designing and building security features into their products.

The PROTECT Act should, but does not, afford complete and immediate export relief for mass market encryption without any complicated oversight. The Act also does not recognize that if a comparable foreign product is available, *any* delay in exports provides a significant advantage to the foreign product.

The PROTECT Act's Relief For 128-Bit AES Products Is Too Little, Too Late

I want to make one final comment regarding the general exportability of mass market products. We support NIST's efforts to establish a new 128-bit Advanced Encryption Standard; however, under the bill, it will not be finalized until 2002. Because the PROTECT Act limits easy exportability of mass market products until the AES is adopted, general distribution of these products will have to wait almost three years. Considering the current speed of technological change, where Internet products are now on three-month product cycle times, and the fact that 128-bit comparable foreign encryption is currently available, this is an eternity in Internet time. Law enforcement and national security interests have known for a long time that ubiquitous use of strong encryption by consumers worldwide is just around the corner. They cannot hope to continue to delay the world from using strong encryption according to their timeframe.

The Time For Action Is Now

To keep American vendors on a level international playing field and American computer users adequately protected, U.S. export controls must be immediately updated to reflect technological and international market realities.

Thank you.